

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

RARICK et al.

Serial No. 10/734,310

Examiner: WANG, Harris

Art Unit: 2139

Atty Docket No. SUNMP349

Filed: December 12, 2003

Date: Feb 13, 2009

For: SYSTEM, METHOD AND  
APPARATUS FOR  
COMBINING  
CRYPTOGRAPHIC HASH  
ALGORITHMS

INVENTOR DECLARATION UNDER 37 CFR 1.132 IN RESPONSE TO  
OFFICE ACTION

I, Leonard D. Rarick, am an inventor in the above referenced application and I hereby declare the following:

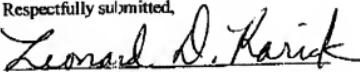
1. 4 to 2 compressors have been known in the art of multiplier arrays for many years as noted in the Oklobdzija reference from 1996.
2. 4 to 2 compressors are defined in the art of multiplier arrays to have a *3 XOR gate delay*.
3. Two sequential full adders have a *4 XOR gate delay*.
4. A single 4 to 2 compressor and two sequential full adders have the same device count and consume approximately the same area on the semiconductor die and consume approximately the same quantity of power.
5. Motivation to improve semiconductor circuit design such as microprocessors and encryption processors, including the hash logic as described in the present application, is driven by power, semiconductor die area or reduction in logic delay.

6. Comparing a 4 to 2 compressor to two sequential full adders shows approximate equal device count, semiconductor die area and power consumption and *only a single XOR gate delay reduction*.
7. 4 to 2 compressors were developed in the art of multiplier arrays because the longest column in the multiplier array uses several 4 to 2 compressors, for example a 64 X 64 multiply array with Booth encoding uses at least four 4 to 2 compressors arranged sequentially (12 XOR gate delay total) to replace eight sequential full adders (16 XOR gate delay total).
8. Using four 4 to 2 compressors arranged sequentially in the example multiplier array *yields a 4 XOR gate delay improvement* as compared to using eight sequential full adders.
9. If a processor (e.g., microprocessor and/or encryption processor) die area and power consumption is not changed and the logic delay of a portion (e.g., hash logic) of the processor is only slightly reduced, *there is substantial motivation to not change* that portion of the processor because that slight reduction in logic delay could require significant redesign of adjacent portions of the processor to compensate for the slight reduction in logic delay.
10. In contrast, using the 4 to 2 compressors in a multiplier array reduces the latency of each column in the multiplier array by *multiple XOR gate delays* as compared to using sequential full adders.
11. In a multiplier array the delay of each column can be additive and therefore the reduced logic delay of each column can yield a further reduced logic delay of the entire multiplier array.
12. These logic delay reductions in the columns of the multiplier array provides the motivation to use 4 to 2 compressors in multiplier arrays because the improvement is very significant – multiple gate delays and these XOR gate delays can be a full clock cycle or more improvement in timing.
13. In hash function logic, as in the present application, the 4 to 2 compressors are *not known* to be used even though the 4 to 2 compressor logic architecture has been known for many years in other art (e.g., multiplier arrays) as noted in the Oklobdzija reference from 1996.

14. The relatively minor improvement in logic delay in only a hash logic portion of a processor provides motivation *to not use* 4 to 2 compressors even if the 4 to 2 compressor was known in the art of hash function logic.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Respectfully submitted,

  
Leonard D. Rarick  
Inventor

Dated: February 13, 2009